AuthentiDate™

The Trusted Content Authority

AuthentiDate 101

An AuthentiDate White Paper
Version 1.0

AuthentiDate, Inc.
2 World Financial Center
225 Liberty Street, 43rd Floor
New York, NY 10281
212-329-1100
www.authentidate.com

Contents

Introduction

What is AuthentiDate?

- (N.) A product that automates the process of authenticating both the **content** and **creation time** of any type of electronic file (such as documents, emails, receipts, pictures, audio and video clips, etc.) that is stored or transmitted over any type of network. *E.g., Have you considered integrating AuthentiDate as part of your IT security solution?*
- (V.) The act of authenticating a file with AuthentiDate. *E.g., I recommend that you Authentidate your confidential Human Resource files as soon as possible.*

About This White Paper

The purpose of this White Paper is to introduce you to the conceptual and technical components of AuthentiDate, an application that can control or mitigate risks associated with the use of electronic files and e-transactions for conducting business.

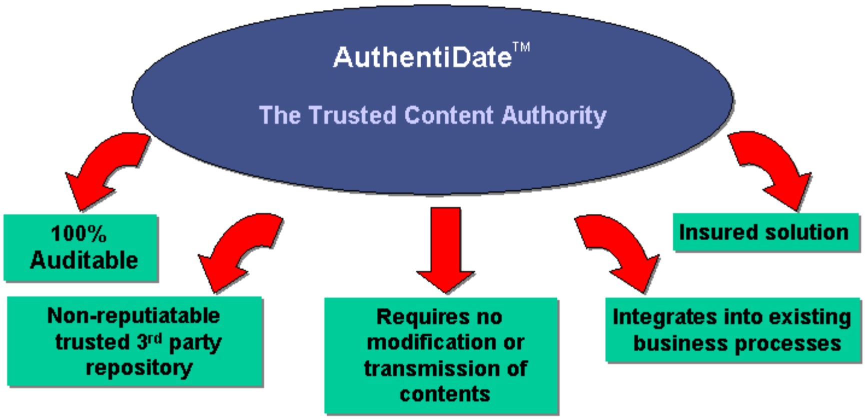
This White Paper consists of five sections:

- The Trusted Content Authority
- The AuthentiDate Framework
- How AuthentiDate Works
- AuthentiDate Technology
- Pending Patents.

The Trusted Content Authority

What is a "Trusted Content Authority"?

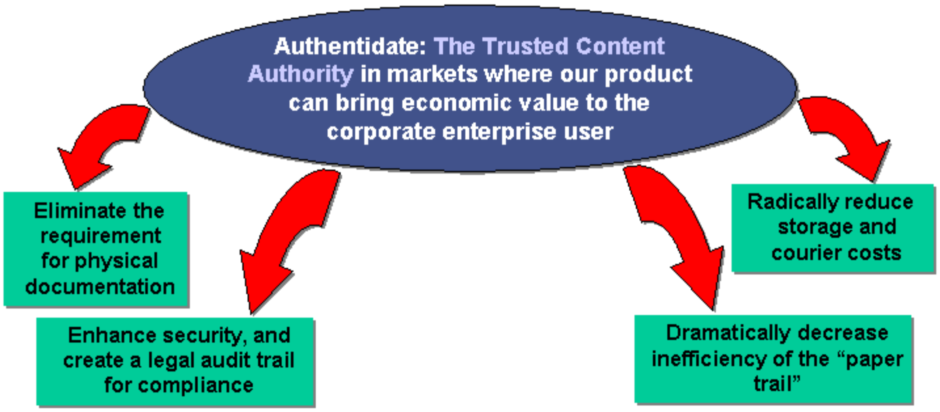
The concept of AuthentiDate as the **Trusted Content Authority** is characterized as follows:


AuthentiDate™
The Trusted Content Authority
100% Auditable
Non-reputiatable trusted 3rd party repository
Requires no modification or transmission of contents
Integrates into existing business processes
Insured solution

- **100% Auditable.** AuthentiDate stores the hash code and time stamp of each item you Authentidate, allowing you to audit with ease and confidence.
- **Non-reputiatable trusted 3rd party repository.** AuthentiDate acts as a neutral 3rd party repository of your Authentidated item's hash code and time stamp, guaranteeing non-repudiation.
- **Requires no modification or transmission of contents.** It's easy to create Scan Profiles that automatically Authentidate files in your specified network folders. You don't have to do anything to your files, or bother with manual transmission.
- **Integrates into existing business processes.** Implementing AuthentiDate as part of your network security and content authentication solution **never** means hours or days of downtime. Installing and maintaining AuthentiDate is easy, the product is transparent to your users — i.e., if you create user Scan Profiles, your users don't even have to know their files are being Authentidated! You can also easily integrate AuthentiDate into your proprietary software via the SDK, explained in our documentation.
- **Insured solution.** AuthentiDate is the world's Trusted Content Authority — it's what we do, and who we are. In fact, we're we're so confident in our product that we back up each AuthentiDate stamp with liability coverage. In other words, AuthentiDate **guarantees** every transaction it processes as well as the possibility of any AuthentiDate stamp that is questioned in the context of a legal proceeding to prove authenticity.

Trusted Content Authority Benefits

Maybe we can save your company millions on lawsuits stemming from fraud and non-authenticated data. Maybe we'll just help you get a good night's sleep. In any case, the benefits of a **Trusted Content Authority** are abundant.



Authentidate: The Trusted Content Authority in markets where our product can bring economic value to the corporate enterprise user

Eliminate the requirement for physical documentation

Enhance security, and create a legal audit trail for compliance

Radically reduce storage and courier costs

Dramatically decrease inefficiency of the "paper trail"

- **Eliminate the requirement for physical documentation.** With AuthentiDate, you can actualize the dream of a "paperless" office. For example, if one of your vendors disputes the authenticity of an old invoice, you don't need to deal with the headaches (and associated costs and storage space) of digging through boxes of paper. In fact, the only space you'll need is a few kilobytes of disk space to store your AuthentiDate receipt verifying the original file's hash code and time stamp.
- **Enhance security, and create a legal audit trail for compliance.** What's probably the first topic your vendors, customers, and auditors want to discuss when assessing your company's technical infrastructure? **Security**. Every day trade magazines and industry web sites report horror stories of data sabotage, electronic identity theft, and frivolous lawsuits that cannot be combated due to lost or manipulated digitized content. Security is a legitimate concern for any business that deals with digitized files, from email to e-commerce. End your security woes (and send your auditors home early) by making AuthentiDate — the Trusted Content Authority — the backbone of your IT security infrastructure.
- **Dramatically decrease inefficiency of the "paper trail".** Your AuthentiDate stamp irrefutably proves the contents (the "what") and the exact time (the "when") of any digitized file. Instead of winding detours and crossroads, your paper trail ends with a stop sign — the Trusted Content Authority.
- **Radically reduce storage and courier costs.** You can spend tens of thousands of dollars each month on expensive storage space for boxes of files. You can pay outrageous courier fees simply to add an extra level of security to their transmitted files and complicate the "paper trail". Or you can Authentidate your files for pennies a transmission, and drastically slash costs.

The AuthentiDate Framework

Our Electronic World

There is no question that the world has become electronically connected. We live in a generation characterized by distributed, business-critical transmission of **electronic files**.

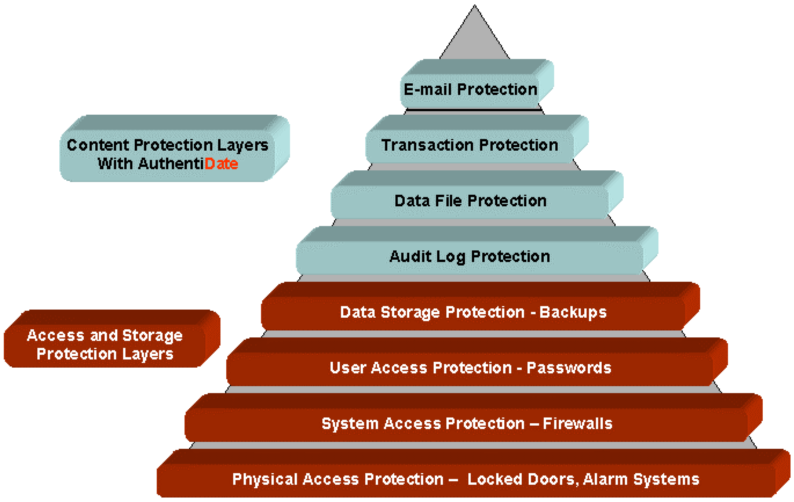
The Internet is becoming more and more critical to these operations through intranets (employees), extranets (trading partners), and the World Wide Web (customers and prospects).

As the volume and variety of data transmitted and stored electronically increases, so too does the potential for fraud. Consequently, many firms' focus is turning towards authenticity. Electronic images can be manipulated and resaved with little effort, calling into question the authenticity of **any** electronic file, including:

- documents
- medical records
- digital video
- photographs
- audio
- spreadsheets
- *and more…*

The AuthentiDate Security Pyramid

The AuthentiDate security pyramid illustrates the ways in which AuthentiDate "builds upon" your physical and electronic security model.


E-mail Protection
Content Protection Layers With AuthentiDate
Transaction Protection
Data File Protection
Audit Log Protection
Data Storage Protection - Backups
Access and Storage Protection Layers
User Access Protection - Passwords
System Access Protection – Firewalls
Physical Access Protection – Locked Doors, Alarm Systems

When using any form of communication, there are a number of security risks. The four **key risks** are that someone will:

- intercept a message and read its contents
- send a message under someone else's name and signature
- change the contents of a message
- deny sending a message.

To reduce these risks, four security services have evolved over time:

- **Confidentiality.** Evidence that the contents of the message have not been disclosed to third parties.

  AuthentiDate does not store your original content — only a time-stamped hash code that matches to the receipt of your original content. In other words, your original content is kept completely confidential.

- **Authenticity.** A guarantee that a message really has come from the person who claims to have sent it.

  Again, AuthentiDate can verify the authentic "who" of any electronic transaction with a server-level certificate. For customers that do have a PKI in place, AuthentiDate's PKI can integrate with the PKI toolkits of major PKI vendors to authenticate content down to the level of a client user's user-level certificate.

- **Integrity.** Proof that the message contents have not been altered, deliberately or accidentally, during transmission.

  Matching your time-stamped, hash-coded original message contents with the database-stored matching time-stamped hash code verifies (or refutes) the integrity of your original message contents.

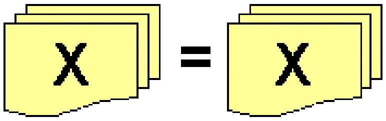
- **Non-repudiation.** In general terms, **non-repudiation** crypto-technically refers to a service that *provides proof of the integrity and origin of data*, both in an *unforgeable relationship*, which can be verified by any third party at any time; or an authentication that with high assurance can be asserted to be genuine, and *that can not subsequently be refuted.*[1]

  Matching your time-stamped, hash-coded original message contents with the database-stored matching time-stamped hash code also guarantees non-repudiation.

[1] W. Caelli, D. Longley, and M. Shain, 1991. *Information Security Handbook.* London: Macmillan.

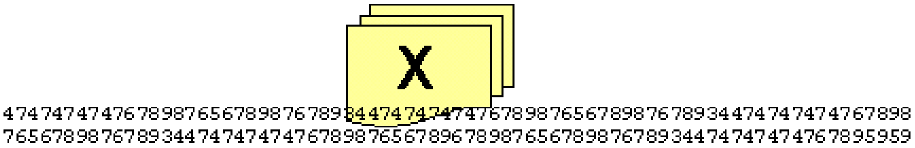
Content Authentication and One-Way Hash Functions

Definition. Content authentication is the process of determining whether or not a file has been altered or tampered with.



A fundamental pre-requisite for understanding how the content authentication procedure works is the concept of one-way hash functions.

Definition. One-way hash functions produce fixed length numbers, often referred to as "file signatures", "hash values" or "message digests", that uniquely represent (is sufficient to identify) a single piece of digital data. File signatures are unique in the sense that two different pieces of data, when run through a one-way hash function, do not statistically create the same file signature. In other words, one-way hash functions verify **"what"** the contents of a transaction are.

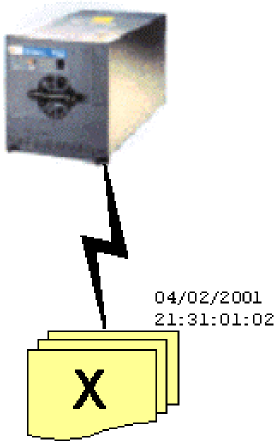


The length of the number is typically 128 bits and can go as high as 160 bits, but longer bit strings can be used for greater security (the longer the bit string, the less likely two different files could produce the same number).

And because the hash functions are 'one-way', no portion of the original data can be reconstructed from the file signature (in the same way an individual cannot be "reconstructed" from his signature or fingerprint).

Time-Stamping

Definition. **Time-stamping** is a set of techniques using cryptography algorithms, enabling one to ascertain whether an electronic document was created or signed at (or before) a certain time. In other words, time-stamping verifies **"when"** a transaction occurred.



In practice, most time-stamping systems use a trusted third party called a Time-Stamping Authority (TSA). A time-stamp is a digital attestation of the TSA that an identified electronic document has been presented to the TSA at a certain time.

Techniques to ensure that the TSA is always appending the correct time are somewhat technical, but the basic idea is that the TSA has to do certain things that can be easily 'audited' and any falsifications (resulting from the TSA or anyone else) would be easily and quickly detectable and traceable.

Certificate Authorities and Digital Certificates

Definition. **Certificate authorities (CAs)** are the digital world's equivalent of passport offices. They issue digital certificates and validate the holder's identity and authority.

CAs embed an individual's or an organization's public key along with other identifying information into each digital certificate and then cryptographically "sign" it as a tamper-proof seal, verifying the integrity of the data within it and validating its use.

Definition. **Digital certificates** authenticate that their holders— people, web sites, and even network resources such as routers— are truly who or what they claim to be. They also protect data exchanged online from theft or tampering.

There are two types of digital certificates that are important when building secure solutions:

- **server-level certificates**
- **user-level certificates**.

Public Key Infrastructure (PKI)

> **Definition. Public-key infrastructure (PKI)** is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their electronic files on the Internet.

PKIs integrate **digital certificates**, **public-key cryptography**, and **certificate authorities (CAs)** into a total, enterprise-wide network security architecture.

A typical enterprise's PKI encompasses:

- the issuance of digital certificates to individual users and servers
- end user enrollment software
- integration with corporate certificate
- directories; tools for managing, renewing, and revoking certificates
- related services and support.

Is AuthentiDate a PKI Product?

No. AuthentiDate is *complementary* to PKI.

In fact, we partner with several leading PKI solution providers.

PKI is a method of strong user-level authentication. Again, PKI is very good at proving **who** the two parties to a transaction are.

AuthentiDate, on the other hand, is primarily concerned with proving **what** a file contains and **when** it was created.

Since AuthentiDate uses PKI to authenticate the SSL connection between the Local Server and the AuthentiDate Central Server, it uses PKI to prove **who** the AuthentiDate stamp comes from and then proves **what** and **when** with our proprietary AuthentiDate technique.

In addition, each AuthentiDate transaction is authenticated using PKI certificates, and stored in our database as a digital certificate, signed by both parties.

How Do I Use AuthentiDate if I Don't (or Do) Have Full PKI?

AuthentiDate has its own PKI technology built in. Customers who:

- **don't** have PKI installed can use a **server-level certificate** for content authentication
- **do** have PKI in place can use their PKI vendor's toolkit to integrate with AuthentiDate's PKI and authenticate content at the **user-level certificate** level.

Adherence to PKI Standards

AuthentiDate's products fully embrace relevant PKI and IETF standards. These include:

- **Digital Certificates.** AuthentiDate uses Digital Certificates for strong authentication of both the customer and the AuthentiDate Central Server. At the customer level, the customer's private key is used to sign the hash of the file.

  At the Central Server level, the Central Server's private key is used to resign the combined certificate containing the hash of the file and the secure time stamp.

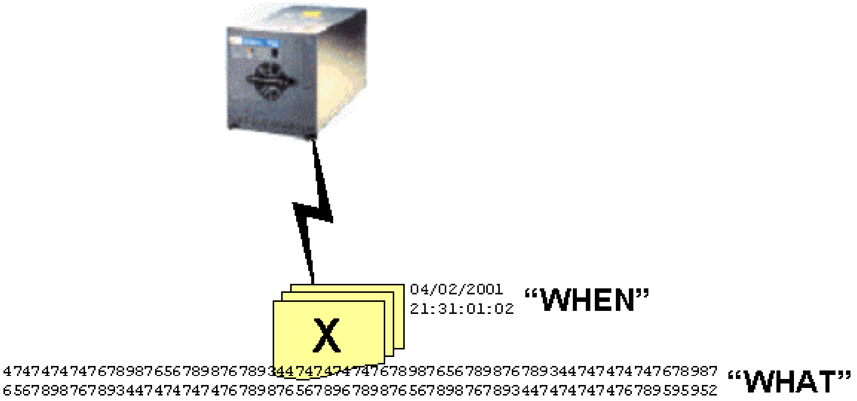
  Since the certificate is signed by both parties, it becomes a legally binding signed document under the new digital signature laws, providing the strongest possible level of non-repudiation to the transaction.
- **Secure Socket Layers.** AuthentiDate uses SSL for secure communications between the customer and the Central Server. Server-level digital certificates are used to authenticate the SSL connection.

How AuthentiDate Works

Overview

So how does AuthentiDate fit into the framework described in the previous section?

Again, using the techniques and security technology outlined in this section, AuthentiDate verifies the content (the "**what**") of any electronic file, and the time (**"when")** the file verification occurred.



Note: AuthentiDate can also verify the authentic **"who"** of any electronic transaction with a server-level certificate. For customers that do have a PKI in place, AuthentiDate's PKI can integrate with the PKI toolkits of major PKI vendors to authenticate content down to the level of a client user's user-level certificate.

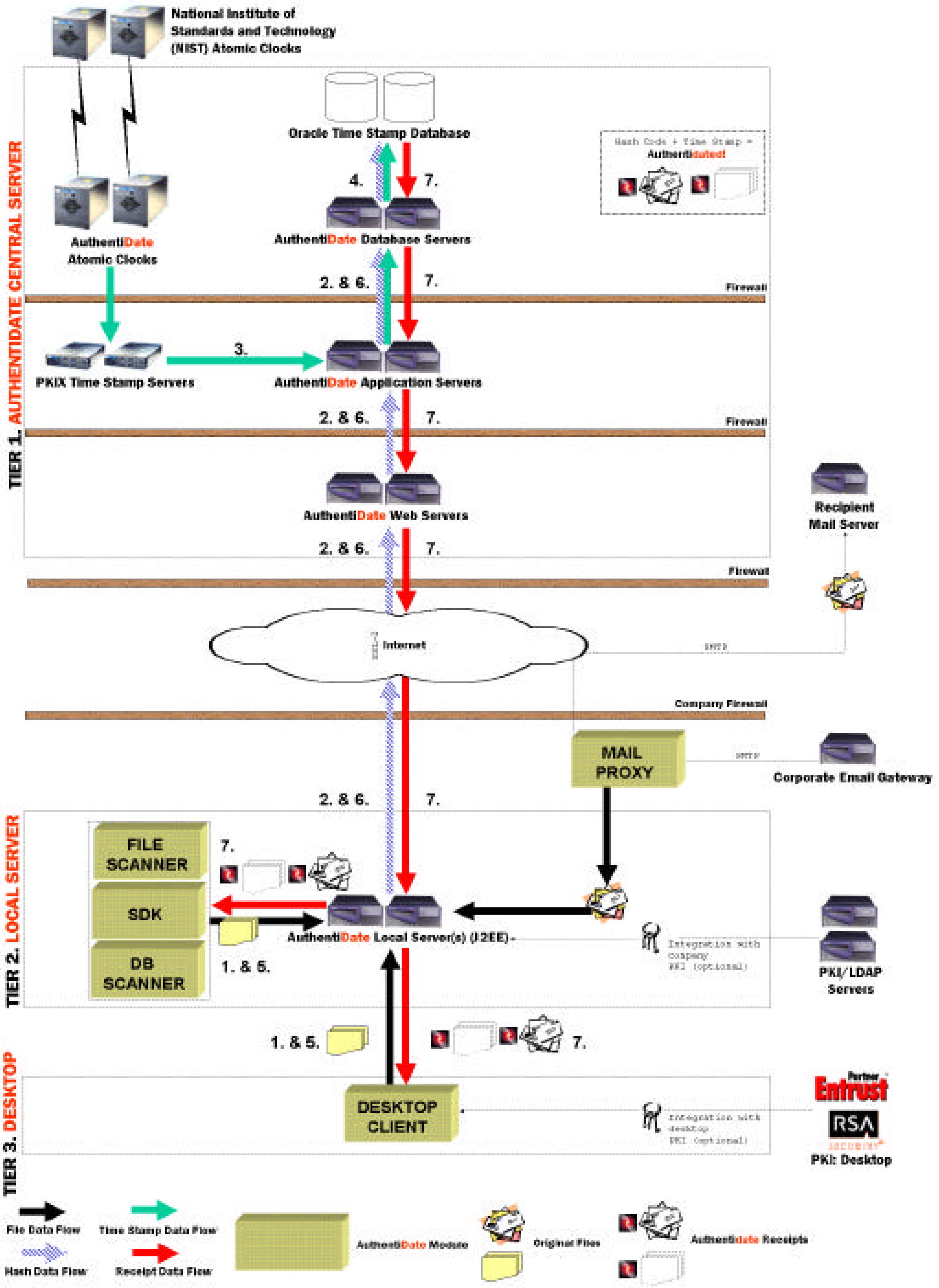
Our technology creates, effectively, an insurance policy for large corporations who rely on the efficiency of the Internet for document transmission within and external to the enterprise.

AuthentiDate, Inc. employs a secure clock, connected to the National Institute of Standards Technology (N.I.S.T's). A Trusted Time Stamp is obtained from N.I.S.T and signed to the unique hash code (associated with each customer's original file) to produce a combined **AuthentiDate Stamp**.

The AuthentiDate Stamp **cannot** be changed by end users— or even by AuthentiDate, Inc.

The next two sections illustrate and describe the process flow of an Authentidated file, as well as the product's three-tier technical architecture.

Process Flow ¾ Illustrated



Note: Also see the "Technology" section of this White Paper for more information on system requirements, AuthentiDate server technology, and the AuthentiDate modules.

Process Flow ¾ Described

STEP	DESCRIPTION
1.	Data files are submitted to AuthentiDate from the Desktop Client or Local Server AuthentiDate Modules.
2.	The Local Server creates a hash code, which is signed and sent to the AuthentiDate Central Server.
3.	A Trusted Time Stamp is obtained from N.I.S.T and signed to the hash code to produce a combined AuthentiDate Stamp.
4.	This combined AuthentiDate Stamp is stored in the Oracle Time Stamp Database, and a receipt is returned to the customer.
5.	At a later date, a data file is submitted to the Local Server for verification.
6.	The hash code is re-computed. AuthentiDate searches the Oracle Time Stamp Database for a stored receipt with a matching hash code.
7.	The matching receipt (with Trusted Time Stamp and matching hash code) is returned to the customer — irrefutably proving the file confidentiality, authenticity, integrity, and non-repudiation.

AuthentiDate Technology

System Requirements

System requirements for the AuthentiDate Local Server are as follows:

- Intel P2 400 processor or better
- Windows 2000 or Windows NT 4.0 (or later)
- 128 MB of RAM
- 500 MB of disk space.

Server Technology

- **Oracle Time Stamp Database Servers.** Oracle supports parallel servers to split the database-processing load over as many servers as are required to perform requested database-processing transactions.

  Oracle's Parallel Server and replication capabilities also make the database scaleable to high volumes.

  In addition, Oracle's replication capabilities support multiple, geographically-distributed AuthentiDate Central Server tiers for higher redundancy and faster response times.

- **Weblogic Application Servers.** Weblogic ensures the application can be scaled to handle virtually unlimited volumes by allowing it to run on multiple processors and systems.

- **Apache Web Servers.** AuthentiDate's web servers are hosted in a secure server environment, operated by ATT&T, one of the worldwide leading IT Service companies.

AuthentiDate Modules

In simplest terms, the **AuthentiDate modules** allow you to Authentidate your files. There are five modules, explained in the matrix below.

MODULE	EXPLANATION
Desktop Client	Consists of two parts: • **MS Office add-ins** integrate a *File > Save and Authentidate* menu option to your Office applications — i.e., Excel, Word, PowerPoint. • **“Authentidate Now!”** — a Windows Explorer extension — allows you to right-click any file in Windows Explorer and Authentidate it.
File Scanner	Allows you to create user **Scan Profiles**. A Scan Profile is a set of instructions that specifies which file (or group of files) you want Authentidated. The Scan Profile instructions are stored and executed based on the frequency schedule specified for that Scan Profile. The file(s) or folders you specify must either exist on the LAN or sharable on your LAN.
SDK	The **Software Developer’s Kit (SDK)** is designed to permit you to integrate AuthentiDate capabilities (specifically, two Java classes) into any software applications you are developing or maintaining.
Mail Proxy	TBA.
DB Scanner	

Verifying and Publishing Your Authentidated Files

After you have Authentidated a file, it's easy to log in to your account to verify both the original hash code and time stamp.

If you store the file on your own computer, you can send it to AuthentiDate again, and we will compare it to the registered file. If the file has not been altered, the AuthentiDate Stamp (hash code and time stamp) will match, providing verification.

You can also publish your Authentidated file as *Universal Global*? allowing **anyone** to verify its Authentidated status.

Appendix A - Pending Patents

Following is a list of pending AuthentiDate patents, including title, description, serial number, and status.

TITLE	DESCRIPTION	SERIAL #	STATUS
"Digital Image Authentication By Secure Image Marking"	Patent filed with the World Intellectual Property Organization (WIPO).	US00/05098	Patent pending; Filed: 2/24/00
"Computer Networked System and Method of Digital File Management and Authentication"	Web-based authentication including transmitting, uploading, archiving, and verifying content over the internet to a secure remote location. Based on the Personal Edition.	09/562,735	Patent pending; Filed:05/01/00
"Computer Networked System and Method of Digital File Management and Authentication Over Network"	High volume, secure and auditable method to create digital signatures, time-stamp, with third-party storage of cryptographically signed information. Allows seamless integration into existing client architecture including standard PKI. Based on the Enterprise Edition.	09/729,411 CIP for 09/562,735	Patent pending; Filed:12/04/00
"Computer Networked System and Method of Digital File Management and Authentication of Memorabilia"	Covers the use of AuthentiDate technology for authenticating autographs, memorabilia, and other collectibles.	TBD	Final internal review

Appendix B - Transaction Insurance Guarantees Every AuthentiDate Stamp

Liability coverage allows AuthentiDate to **guarantee** every transaction it processes as well as the possibility of any AuthentiDate stamp that is questioned in the context of a legal proceeding to prove authenticity. Specifics of the insurance policy include:

- **$5,000,000** maximum liability coverage for failure of AuthentiDate's security that causes un-authorized use or access, disclosure of confidential or private information, transmission of computer virus or denial of service to customers or clients.
- **$5,000,000** maximum media coverage for each claim alleging content-based injuries such as libel, slander or defamation, copyright, title or trademark infringement or invasion of privacy.
- **$5,000,000** maximum extortion coverage for investigation and settlement of bona-fide cyber-attack threats.
- **$5,000,000** maximum asset and income protection to cover property losses involving intangible assets such as credit card numbers, customer list and business strategies (Intellectual Property).

For each category of coverage, expense is subject to the limits of **$100,000** per occurrence.